

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-140896

(43)Date of publication of application : 02.06.1995

(51)Int.Cl.

G09C 1/00

G06F 12/14

(21)Application number : 05-314466

(71)Applicant : HITACHI LTD
HITACHI SOFTWARE ENG CO LTD

(22)Date of filing : 19.11.1993

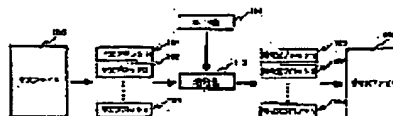
(72)Inventor : SUZAKI SEIICHI
TAKARAGI KAZUO
NAKAMURA TERUO
NOTOMI MASAHIITO

(54) FILE CIPHERING METHOD AND ITS DEVICE

(57)Abstract:

PURPOSE: To adequately cipher a file to be written into a memory device without depending on the kind of an application program by which the file is formed.

CONSTITUTION: The ordinary text file 100 is divided by n to the smallest data size at which data transaction between the data region on a memory to be used by the application program and a disk buffer is possible, by which n -pieces of ordinary text blocks 101 to 103 are formed. Next, n -pieces of these ordinary text blocks 101 to 103 are respectively separately ciphered by a user key 104 and n -pieces of cipher text blocks 105 to 107 are formed. Finally, the formed n -pieces of these cipher text blocks 105 to 107 are connected to obtain a cipher text file 108. Then, the application program ciphers the ordinary text file by each of the smallest data size at which a partial operation, such as superscription, of the file is possible and, therefore, the correct deciphering to the original ordinary text file is possible at any time even if any operation is executed by the application program.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision]

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-140896

(43) 公開日 平成7年(1995)6月2日

| | | | | |
|---------------------------|---------|---------|-----|--------|
| (51) Int.Cl. ⁶ | 識別記号 | 庁内整理番号 | F I | 技術表示箇所 |
| G 0 9 C 1/00 | | 9364-5L | | |
| G 0 6 F 12/14 | 3 2 0 B | | | |

審査請求 未請求 請求項の数30 F D (全 14 F)

(21) 出願番号 特願平5-314466

(22) 出願日 平成5年(1993)11月19日

(71) 出願人 000005108

株式会社日立製作所
東京都千代田区神田駿河台四丁目6番地

(71) 出願人 000233055

日立ソフトウェアエンジニアリング株式会
社
神奈川県横浜市中区尾上町6丁目81番地

(72) 発明者 洲崎 誠一

神奈川県川崎市麻生区王禅寺1000番地 株
式会社日立製作所システム開発研究所内

(74) 代理人 弁理士 矢島 保夫

最終頁に続く

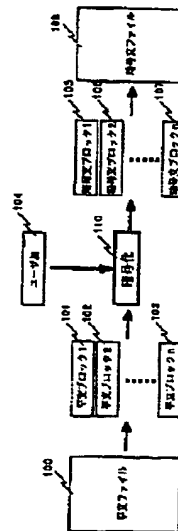
(54) 【発明の名称】 ファイル暗号方法及びその装置

(57) 【要約】

【目的】 ファイルを作成したアプリケーションプログラムの種類に依らず、記憶装置に書き込むファイルを適切に暗号化する。

【構成】 まず、アプリケーションプログラムが使用するメモリ上のデータ領域とディスクバッファとの間でデータのやり取りを行なうことができる最も小さなデータサイズに、平文ファイル100をn分割し、n個の平文ブロック101、102、103を生成する。次に、このn個の平文ブロック101、102、103を、ユーザ鍵104でそれぞれ別々に暗号化し、n個の暗号文ブロック105、106、107を生成する。最後に、生成されたn個の暗号文ブロック105、106、107を連結して、暗号文ファイル108を得る。

【効果】 アプリケーションプログラムが、ファイルに対して、上書き等の部分的操作が可能な最も小さなデータサイズ毎に平文ファイルを暗号化するので、アプリケーションプログラムでどのような操作が行なわれようと、いつでも元の平文ファイルに正しく復元することができる。



-1-

(2) 特開平7-140896

【特許請求の範囲】

【請求項1】与えられた平文ファイルを、与えられたユーザ鍵で暗号化し、得られた暗号文ファイルを記憶装置に記憶するとともに、外部からのファイルアクセス指示に応じて該記憶装置にアクセスするファイル暗号方法であって、

与えられた平文ファイルの書き込みの手順が、書き込みを指示された平文ファイルを、外部からファイルアクセスを指示される際の最も小さなデータサイズまたはそれより小さなデータサイズを単位として分割し、複数の平文ブロックを生成するステップと、与えられたユーザ鍵を用いて、該複数の平文ブロックをそれぞれ別々に暗号化し、複数の暗号文ブロックを生成するステップと、

該複数の暗号文ブロックを連結して暗号文ファイルを生成するステップと、

該暗号文ファイルを前記記憶装置に書き込むステップとを備えたことを特徴とするファイル暗号方法。

【請求項2】請求項1に記載のファイル暗号方法において、さらに、

指定された平文ファイルの読み出しの手順が、該指定された平文ファイルに対応する暗号文ファイルを前記記憶装置から読み出すステップと、

読み出した暗号文ファイルを複数の暗号文ブロックに分割し、その際、各暗号文ブロックを復号すると元の複数の平文ブロックが得られるような所定の大きさで分割するステップと、

与えられたユーザ鍵を用いて、該複数の暗号文ブロックをそれぞれ別々に復号し、複数の平文ブロックを生成するステップと、

該複数の平文ブロックを連結して平文ファイルを生成するステップと、

該平文ファイルを出力するステップとを備えたことを特徴とするファイル暗号方法。

【請求項3】請求項1に記載のファイル暗号方法において、さらに、

ユーザ鍵と、平文ファイルを特定する情報と、該平文ファイル内の位置と、該位置に上書きすべき平文データとが与えられたときに、該平文データを上書きする手順が、

上書きを指示された平文データを、前記平文ファイルの分割と同じデータサイズで分割し、複数の上書き用平文ブロックを生成するステップと、

与えられたユーザ鍵を用いて、該複数の上書き用平文ブロックをそれぞれ別々に暗号化し、複数の上書き用暗号文ブロックを生成するステップと、

該複数の上書き用暗号文ブロックを連結して上書き用暗号文データを生成するステップと、

該上書き用暗号文データを、前記記憶装置の上書きを指示された平文ファイルに対応する暗号文ファイルの上

書きを指示された位置に上書きするステップとを備えたことを特徴とするファイル暗号方法。

【請求項4】与えられた平文ファイルを、与えられたユーザ鍵で暗号化し、得られた暗号文ファイルを記憶装置に記憶するとともに、外部からのファイルアクセス指示に応じて該記憶装置にアクセスするファイル暗号方法であって、

与えられた平文ファイルの書き込みの手順が、書き込みを指示された平文ファイルを、外部からファイルアクセスを指示される際の最も小さなデータサイズまたはそれより小さなデータサイズを単位として分割し、複数の平文ブロックを生成するステップと、

与えられたユーザ鍵と前記複数の平文ブロックの各々に固有の情報とから、各平文ブロックにそれぞれ対応する秘密鍵であるデータ鍵を生成するステップと、

該複数のデータ鍵を用いて、前記複数の平文ブロックをそれぞれ別々に暗号化し、複数の暗号文ブロックを生成するステップと、

該複数の暗号文ブロックを連結して暗号文ファイルを生成するステップと、

該暗号文ファイルを前記記憶装置に書き込むステップとを備えたことを特徴とするファイル暗号方法。

【請求項5】請求項4に記載のファイル暗号方法において、さらに、

指定された平文ファイルの読み出しの手順が、該指定された平文ファイルに対応する暗号文ファイルを前記記憶装置から読み出すステップと、

読み出した暗号文ファイルを複数の暗号文ブロックに分割し、その際、各暗号文ブロックを復号すると元の複数の平文ブロックが得られるような所定の大きさで分割するステップと、

与えられたユーザ鍵と前記複数の平文ブロックの各々に固有の情報とから、各平文ブロックにそれぞれ対応するデータ鍵を生成するステップと、

該複数のデータ鍵を用いて、前記複数の暗号文ブロックをそれぞれ別々に復号し、複数の平文ブロックを生成するステップと、

該複数の平文ブロックを連結して平文ファイルを生成するステップと、

該平文ファイルを出力するステップとを備えたことを特徴とするファイル暗号方法。

【請求項6】請求項4に記載のファイル暗号方法において、さらに、

ユーザ鍵と、平文ファイルを特定する情報と、該平文ファイル内の位置と、該位置に上書きすべき平文データとが与えられたときに、該平文データを上書きする手順が、

上書きを指示された平文データを、前記平文ファイルの分割と同じデータサイズで分割し、複数の上書き用平文ブロックを生成するステップと、

(3) 特開平7-140896

与えられたユーザ鍵と前記複数個の上書き用平文ブロックの各々に固有の情報とから、各上書き用平文ブロックにそれぞれ対応するデータ鍵を生成するステップと、該複数個のデータ鍵を用いて、該複数個の上書き用平文ブロックをそれぞれ別々に暗号化し、複数個の上書き用暗号文ブロックを生成するステップと、該複数個の上書き用暗号文ブロックを連結して上書き用暗号文データを生成するステップと、該暗号文データを、前記記憶装置の上書きを指示された平文ファイルに対応する暗号文ファイルの上書きを指示された位置に上書きするステップとを備えたことを特徴とするファイル暗号方法。

【請求項7】請求項4から6のいずれか1つに記載のファイル暗号方法において、前記複数個の平文ブロックの各々に固有の情報が、平文ファイルの先頭からその平文ブロックまでのオフセットであることを特徴とするファイル暗号方法。

【請求項8】請求項1から7のいずれか1つに記載のファイル暗号方法において、前記暗号化および復号化は、平文ブロックと暗号文ブロックのデータサイズが同じとなるアルゴリズムを用いて行うことを特徴とするファイル暗号方法。

【請求項9】請求項1から8のいずれか1つに記載のファイル暗号方法において、前記分割、暗号化および復号化は、上位のアプリケーションからアクセスできないワーク領域の上で行うことを特徴とするファイル暗号方法。

【請求項10】請求項1から9のいずれか1つに記載のファイル暗号方法において、前記ユーザ鍵は、あらかじめユーザに対して配布された個人用記憶媒体に格納されているユーザ鍵を読み出して用いることを特徴とするファイル暗号方法。

【請求項11】請求項10に記載のファイル暗号方法において、前記個人用記憶媒体には、前記ユーザ鍵と共に、該個人用記憶媒体を所有するユーザを識別するためのユーザ識別子とパスワードとが記憶されており、該ユーザ識別子とパスワードを使って本人確認処理を行ない、正しいユーザであることが確認されたときにだけ、前記個人用記憶媒体からユーザ鍵を読み出せることを特徴とするファイル暗号方法。

【請求項12】請求項11に記載のファイル暗号方法において、前記パスワードの代わりに生物学的特徴によって本人確認処理を行なうことを特徴とするファイル暗号方法。

【請求項13】請求項10から12のいずれか1つに記載のファイル暗号方法において、前記記憶媒体がICカードであることを特徴とするファイル暗号方法。

【請求項14】請求項10から12のいずれか1つに記載のファイル暗号方法において、前記記憶媒体がフロッピーディスクであることを特徴とするファイル暗号方

法。

【請求項15】請求項1から14のいずれか1つに記載のファイル暗号方法において、前記記憶装置が通信網を介して接続されており、前記暗号文ファイルや上書き用暗号文データの書き込みおよび読み出しは、該通信網を介して行われることを特徴とするファイル暗号方法。

【請求項16】暗号化したファイルを記憶するための記憶装置を備えるとともに、外部からのファイルアクセス指示に応じてファイルアクセスのサービスを実行するファイル暗号装置であって、

書き込みを指示された平文ファイルを、外部からファイルアクセスを指示される際の最も小さなデータサイズまたはそれより小さなデータサイズを単位として分割し、複数個の平文ブロックを生成する手段と、

与えられたユーザ鍵を用いて、該複数個の平文ブロックをそれぞれ別々に暗号化し、複数個の暗号文ブロックを生成する手段と、

該複数個の暗号文ブロックを連結して暗号文ファイルを生成する手段と、

該暗号文ファイルを前記記憶装置に書き込む手段とを備えたことを特徴とするファイル暗号装置。

【請求項17】請求項16に記載のファイル暗号装置において、さらに、

読み出しを指定された平文ファイルに対応する暗号文ファイルを前記記憶装置から読み出す手段と、

読み出した暗号文ファイルを複数個の暗号文ブロックに分割し、その際、各暗号文ブロックを復号すると元の複数個の平文ブロックが得られるような所定の大きさで分割する手段と、

与えられたユーザ鍵を用いて、該複数個の暗号文ブロックをそれぞれ別々に復号し、複数個の平文ブロックを生成する手段と、

該複数個の平文ブロックを連結して平文ファイルを生成する手段と、

該平文ファイルを出力する手段とを備えたことを特徴とするファイル暗号装置。

【請求項18】請求項16に記載のファイル暗号装置において、さらに、

ユーザ鍵と、平文ファイルを特定する情報と、該平文ファイル内の位置と、該位置に上書きすべき平文データとを入力する手段と、

上書きを指示された平文データを、前記平文ファイルの分割と同じデータサイズで分割し、複数個の上書き用平文ブロックを生成する手段と、

与えられたユーザ鍵を用いて、該複数個の上書き用平文ブロックをそれぞれ別々に暗号化し、複数個の上書き用暗号文ブロックを生成する手段と、

該複数個の上書き用暗号文ブロックを連結して上書き用暗号文データを生成する手段と、

該上書き用暗号文データを、前記記憶装置の上書きを指

5

示された平文ファイルに対応する暗号文ファイルの上書きを指示された位置に上書きする手段とを備えたことを特徴とするファイル暗号装置。

【請求項19】暗号化したファイルを記憶するための記憶装置を備えるとともに、外部からのファイルアクセス指示に応じてファイルアクセスのサービスを実行するファイル暗号装置であって、

書き込みを指示された平文ファイルを、ファイルアクセスを指示される際の最も小さなデータサイズまたはそれより小さなデータサイズを単位として分割し、複数の平文ブロックを生成する手段と、

与えられたユーザ鍵と前記複数の平文ブロックの各々に固有の情報とから、各平文ブロックにそれぞれ対応する秘密鍵であるデータ鍵を生成する手段と、

該複数のデータ鍵を用いて、前記複数の平文ブロックをそれぞれ別々に暗号化し、複数の暗号文ブロックを生成する手段と、

該複数の暗号文ブロックを連結して暗号文ファイルを生成する手段と、

該暗号文ファイルを前記記憶装置に書き込む手段とを備えたことを特徴とするファイル暗号装置。

【請求項20】請求項19に記載のファイル暗号装置において、さらに、

読み出しを指定された平文ファイルに対応する暗号文ファイルを前記記憶装置から読み出す手段と、

読み出した暗号文ファイルを複数の暗号文ブロックに分割し、その際、各暗号文ブロックを復号すると元の複数の平文ブロックが得られるような所定の大きさで分割する手段と、

与えられたユーザ鍵と前記複数の平文ブロックの各々に固有の情報とから、各平文ブロックにそれぞれ対応するデータ鍵を生成する手段と、

該複数のデータ鍵を用いて、前記複数の暗号文ブロックをそれぞれ別々に復号し、複数の平文ブロックを生成する手段と、

該複数の平文ブロックを連結して平文ファイルを生成する手段と、

該平文ファイルを出力する手段とを備えたことを特徴とするファイル暗号装置。

【請求項21】請求項19に記載のファイル暗号装置において、さらに、

ユーザ鍵と、平文ファイルを特定する情報と、該平文ファイル内の位置と、該位置に上書きすべき平文データとを入力する手段と、

上書きを指示された平文データを、前記平文ファイルの分割と同じデータサイズで分割し、複数の上書き用平文ブロックを生成する手段と、

与えられたユーザ鍵と前記複数の上書き用平文ブロックの各々に固有の情報とから、各上書き用平文ブロックにそれぞれ対応するデータ鍵を生成する手段と、

(4)

特開平7-140896

6

該複数のデータ鍵を用いて、該複数の上書き用平文ブロックをそれぞれ別々に暗号化し、複数の上書き用暗号文ブロックを生成する手段と、

該複数の上書き用暗号文ブロックを連結して上書き用暗号文データを生成する手段と、

該上書き用暗号文データを、前記記憶装置の上書きを指示された平文ファイルに対応する暗号文ファイルの上書きを指示された位置に上書きする手段とを備えたことを特徴とするファイル暗号装置。

【請求項22】請求項19から21のいずれか1つに記載のファイル暗号装置において、前記複数の平文ブロックの各々に固有の情報が、平文ファイルの先頭からその平文ブロックまでのオフセットであることを特徴とするファイル暗号装置。

【請求項23】請求項16から22のいずれか1つに記載のファイル暗号装置において、前記ユーザ鍵とデータ鍵を用いて暗号化および復号化を行う各手段は、平文ブロックと暗号文ブロックのデータサイズが同じとなるアルゴリズムを用いて暗号化および復号化を行うことを特徴とするファイル暗号装置。

【請求項24】請求項19から23のいずれか1つに記載のファイル暗号装置において、さらに、上位のアプリケーションからアクセスできないワーク領域を備え、前記分割、暗号化および復号化は該ワーク領域の上で行うことを特徴とするファイル暗号装置。

【請求項25】請求項19から24のいずれか1つに記載のファイル暗号装置において、前記ユーザ鍵は、あらかじめユーザに対して配布された個人用記憶媒体に格納されていることを特徴とするファイル暗号装置。

【請求項26】請求項25に記載のファイル暗号装置において、前記個人用記憶媒体には、前記ユーザ鍵と共に、該個人用記憶媒体を所有するユーザを識別するためのユーザ識別子とパスワードとが記憶されており、該ユーザ識別子とパスワードを使って本人確認処理を行ない、正しいユーザであることが確認されたときにだけ、前記個人用記憶媒体からユーザ鍵を読み出せることを特徴とするファイル暗号装置。

【請求項27】請求項26に記載のファイル暗号装置において、前記パスワードの代わりに生物学的特徴によって本人確認処理を行なう手段を備えたことを特徴とするファイル暗号装置。

【請求項28】請求項25から27のいずれか1つに記載のファイル暗号装置において、前記記憶媒体がICカードであることを特徴とするファイル暗号装置。

【請求項29】請求項25から27のいずれか1つに記載のファイル暗号装置において、前記記憶媒体がフロッピーディスクであることを特徴とするファイル暗号装置。

【請求項30】請求項19から29のいずれか1つに記載のファイル暗号装置において、前記記憶装置が通信網

7

を介して接続されており、前記暗号文ファイルを上書き用暗号文データの書き込みと読み出しは、該通信網を介して行われることを特徴とするファイル暗号装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、パーソナルコンピュータ等の情報処理端末で作成される平文ファイルを選択的に暗号化することができるファイル暗号方法及びそのような暗号方法を適用した情報処理システムに関し、更に詳しくは、平文ファイルを作成するために使用するアプリケーションプログラムの種類に依らず、例えば、既に記憶装置に記憶されている暗号文ファイルの一部を上書きした場合でも、元の平文ファイルに正しく復元することができ、また、通信網を介して別の端末の記憶装置に暗号文ファイルを記憶する場合も自端末の記憶装置の場合と同様の安全性を確保することができるファイル暗号方法及び情報処理システムに関する。

【0002】

【従来の技術】情報機器の発達により、様々な情報が電子的なファイルとして、ハードディスクやフロッピーディスク等の記憶装置に保管されるようになってきている。そのため、機密性の高い情報を含むようなファイルに対しては、暗号化やアクセス制御といったセキュリティ技術を使って情報の保護を行っている。

【0003】一方、ワークステーションやパソコンを端末としたローカルエリアネットワーク（LAN）の普及により、ある端末で作成したファイルを、通信網を介して別の端末の記憶装置に保管する、といったことも行われるようになってきている。

【0004】LANでは、情報は通信回線上を同様に流れている。すなわち、情報の送信元は、送信すべき情報に相手先のアドレスを付して回線に送信し、回線上の全ての端末でこれを受信する。受信した端末では、そのアドレスを参照して、自分宛の情報かどうかをチェックする。したがって、ある端末が同様に送出した情報は、基本的に、どの端末でも受信可能である。そのため、機密性の高い情報を含むようなファイルを通信網を介して別の端末の記憶装置に保管する場合には、自端末の記憶装置に保管する場合と同様に、暗号化やアクセス制御といったセキュリティ技術を使って、適切に保護する必要がある。

【0005】従来の暗号方法については、例えば、「現代暗号理論（著：池野 信一、小山 謙二；発行：社団法人 電子情報通信学会）」に開示されている。

【0006】上記開示例では、平文を数バイト程度のブロックに分割し、各ブロックを同一の暗号鍵で暗号化する。何バイト程度のブロックに分割するかは暗号アルゴリズムの種類によって決まるが、通常は64ビット（8バイト）程度に分割する。

【0007】この方法は、平文を分割した全ての平文ブ

(5)

特開平7-140896

8

ロックの暗号化に同一の暗号鍵を用いるので、同一の平文ブロックは同一の暗号文ブロックに変換される。したがって、暗号文ブロックの出現確率から統計的に元の平文ブロックを類推される危険性がある。そのため、暗号文ブロックを平文ブロックと暗号鍵の値に依存させるだけでなく、暗号化しようとする平文ブロックの前にある前平文ブロックや前暗号文ブロックの値にも依存させて暗号文ブロックを作成する手法も広く用いられている。

【0008】ところで、アプリケーションプログラムが、記憶装置にファイルを書き込んだり、記憶装置に保管されているファイルを読み取る場合には、通常、次のような手順で行なわれる。

【0009】すなわち、アプリケーションプログラムによって指定されたメモリ上のデータ領域にあるファイルは、オペレーティングシステムの制御のもと、一度、ディスクバッファや通信バッファに転送され、その後、自端末、あるいは別の端末の記憶装置に書き込まれる。同様に、既に自端末、あるいは別の端末の記憶装置に保管されているファイルは、一度、ディスクバッファや通信バッファに転送された後、アプリケーションプログラムによって指定されたメモリ上のデータ領域に読み込まれる。

【0010】ファイル全体ではなく、アプリケーションプログラムを使って、既に自端末、あるいは別の端末の記憶装置に保管されているファイルの一部分のみを修正するような場合にも、ほぼ同様のことが行われる。

【0011】

【発明が解決しようとする課題】ファイルを作成するためのアプリケーションプログラムは多種多様であり、また、ユーザがそれらのアプリケーションプログラムを使用する環境も多岐にわたっている。そのため、アプリケーションプログラムの種類や、それを使用する環境に依らず、ファイルの暗号化を適切に行うことができるようにしたいといった要求がある。

【0012】しかし、上記従来技術では、平文ファイルを数バイト程度のブロックに分割して暗号化するので、アプリケーションプログラムが、既に記憶装置に保管されている暗号文ファイルに対し、それより小さなサイズで部分的に上書きした場合に、ブロック内の他のデータとの相関が壊れてしまい、そのブロック全体を正しく復元することができなくなってしまう。

【0013】また、暗号文ブロックを平文ブロックと暗号鍵の値に依存させるだけでなく、前平文ブロックや前暗号文ブロックの値にも依存させる手法を用いた場合には、上書きにされたブロック以降のブロックは、全て正しく復元することができなくなってしまう。

【0014】そこで、本発明の一つの目的は、ユーザが使用しているアプリケーションプログラムの種類に依らず、例えば、そのアプリケーションプログラムによって、既に記憶装置に記憶されている暗号文ファイルが部

9

分的に上書きされた場合でも、元の平文ファイルに正しく復元することができるファイル暗号方法及び情報処理システムを提供することにある。

【0015】本発明のもう一つの目的は、暗号文ファイルから元の平文ファイルを復元されてしまう危険性の少ないファイル暗号方法及び情報処理システムを提供することにある。

【0016】本発明の更にもう一つの目的は、通信網を介して別の端末の記憶装置にファイルを保管する場合にも、自端末の記憶装置に保管する場合と同様の安全性を確保することができるファイル暗号方法及び情報処理システムを提供することにある。

【0017】

【課題を解決するための手段】上記の目的を達成するため、本発明に係るファイル暗号方法またはその装置は、与えられた平文ファイルを、与えられたユーザ鍵で暗号化し、得られた暗号文ファイルを記憶装置に記憶するとともに、外部からのファイルアクセス指示に応じて該記憶装置にアクセスする方法または装置であって、与えられた平文ファイルの書き込みは、書き込みを指示された平文ファイルを、外部からファイルアクセスを指示される際の最も小さなデータサイズまたはそれより小さなデータサイズを単位として分割し、複数の平文ブロックを生成し、与えられたユーザ鍵を用いて、該複数の平文ブロックをそれぞれ別々に暗号化し、複数の暗号文ブロックを生成し、該複数の暗号文ブロックを連結して暗号文ファイルを生成し、該暗号文ファイルを前記記憶装置に書き込むようにする。

【0018】さらに、指定された平文ファイルの読み出しは、該指定された平文ファイルに対応する暗号文ファイルを前記記憶装置から読み出し、読み出した暗号文ファイルを複数の暗号文ブロックに分割し、その際、各暗号文ブロックを復号すると元の複数の平文ブロックが得られるような所定の大きさで分割するものとし、与えられたユーザ鍵を用いて、該複数の暗号文ブロックをそれぞれ別々に復号し、複数の平文ブロックを生成し、該複数の平文ブロックを連結して平文ファイルを生成し、該平文ファイルを出力するようにする。

【0019】また、ユーザ鍵と、平文ファイルを特定する情報と、該平文ファイル内の位置と、該位置に上書きすべき平文データとが与えられたときに、該平文データの上書きは、上書きを指示された平文データを、前記平文ファイルの分割と同じデータサイズで分割し、複数の上書き用平文ブロックを生成し、与えられたユーザ鍵を用いて、該複数の上書き用平文ブロックをそれぞれ別々に暗号化し、複数の上書き用暗号文ブロックを生成し、該複数の上書き用暗号文ブロックを連結して上書き用暗号文データを生成し、該上書き用暗号文データを、前記記憶装置の上書きを指示された平文ファイルに対応する暗号文ファイルの上書きを指示された位置に上

(6)

特開平7-140896

10

書きするようにする。

【0020】さらに、与えられたユーザ鍵を用いて暗号化および復号化を行うのではなく、各ユーザ毎に異なる秘密数値であるユーザ鍵と、平文ファイルの各ブロックに固有の情報（例えば、ファイルの先頭からのオフセット値）等から平文ブロックと同じ個数のデータ鍵を生成し、そのデータ鍵を使って暗号化するようにしてもよい。

【0021】暗号化および復号化は、平文ブロックと暗号文ブロックのデータサイズが同じとなるアルゴリズムを用いるのがよい。平文ファイル上の位置と暗号文ファイル上の位置との対応が簡単に取れる（平文ブロックの平文ファイル先頭からのオフセットと、その平文ブロックに対応する暗号文ブロックの暗号文ファイル先頭からのオフセットとが、同じ）からである。ただし、本発明では、平文ブロックと暗号文ブロックのデータサイズが同じにならないアルゴリズムを用いてもよい。その場合、平文ファイル内の位置と暗号文ファイル内の位置とが相互に変換できるような関数が特定されることが必要になる。

【0022】分割、暗号化および復号化は、上位のアプリケーションからアクセスできないワーク領域の上で行うとよい。上位のアプリケーションの管理下にある領域でこれらの処理を行うと、アプリケーションによっては該領域のデータをさらに表示する処理などを行うことが考えられるからである。

【0023】ユーザ鍵は、あらかじめユーザに対して配布された個人用記憶媒体に格納されているものを用いるとよい。個人用記憶媒体としては、例えば、ICカードやフロッピーディスクを用いる。

【0024】また、個人用記憶媒体にユーザ鍵と共に、該個人用記憶媒体を所有するユーザを識別するためのユーザ識別子とパスワードとを記憶しておき、該ユーザ識別子とパスワードを使って本人確認処理を行ない、正しいユーザであることが確認されたときにだけ、前記個人用記憶媒体からユーザ鍵を読み出せるようにすれば、さらに情報の安全性を確保できる。本人確認処理は、パスワードの代わりに生物学的特徴によって行うようにしてもよい。

【0025】さらに、暗号文ファイルや暗号文データを、通信網を介して接続された記憶装置に、書き込みおよび読み出しするようにしてもよい。

【0026】

【作用】本発明によれば、使用する暗号アルゴリズムの種類に依存した大きさのブロックに平文ファイルを分割するのではなく、例えばアプリケーションプログラムがそのファイルに対して部分的操作のできるデータサイズと同じ、あるいはそれより小さなブロック毎に暗号化しているので、それぞれの暗号文ブロックには相関がなく、たとえアプリケーションプログラムが、既に記憶装

(7)

特開平 7-140896

11

図に保管されている暗号文ファイルの一部を上書きした場合においても、元の平文ファイルに正しく復元することができる。

【0027】また、各平文ブロックをそれぞれ異なるデータ鍵で暗号化する方法によれば、暗号文ブロックを前平文ブロックや前暗号文ブロックの値に依存させなくても、同一の平文ブロックが、必ずしも同一の暗号文ブロックに変換されることはなくなるため、平文ファイルを乱雑されにくくすることができる。

【0028】さらに、通信網を介して接続された記憶装置に暗号文ファイルや暗号文データの書き込みおよび読み出しするようにすれば、通信網を流れるデータは暗号化されたデータとなるから、自端末の記憶装置に書き込む場合と同様の安全性を確保することができる。

【0029】

【実施例】以下、図面を用いて、本発明の実施例を説明する。なお、以下で説明する図面において、同一の番号は同様の部品・要素を表すものとする。また、これにより本発明が限定されるものではない。

【0030】（実施例1）図1は、本発明の第1の実施例に係るファイル暗号化方法による平文ファイルの暗号化手順を示すブロック図である。図2は、本実施例のファイル暗号化方法を用いた情報処理システムのシステム構成を示すブロック図である。

【0031】まず、図2を参照して、本実施例のシステム構成を説明する。

【0032】図2において、200はワークステーションやパソコン等の端末である。ユーザは、これらの端末を使って種々の作業を行なう。210は、ケーブル211によって端末と接続された記憶装置である。ユーザは、アプリケーションプログラムを使って作成したファイルを、この記憶装置210に記憶させることができる。また、記憶装置210に記憶されているファイルを読み取ることもできる。

【0033】220は、あらかじめ各ユーザに対してそれぞれ1つずつ配布されており、容易に持ち運ぶことができる個人用記憶媒体（例えば、フロッピーディスクやICカード）である。ユーザは、自己の個人用記憶媒体を読み取り装置230に差し込んで、作業を行なう。個人用記憶媒体220は、読み取り装置230とケーブル231とを介して端末200にデータを送る。

【0034】図3は、端末200の内部構成図である。同図に示すように、端末200は、CPU〔中央処理装置〕301と、読み取り装置インタフェース302と、記憶装置インタフェース303と、表示装置304と、入力装置305と、メモリ306とを有している。それらは、バス300によって相互に接続されている。

【0035】CPU301は、種々の演算処理を行なう。読み取り装置インタフェース302は、ケーブル231を介して読み取り装置230から送られてくるデー

12

タを受け取るためのインタフェースである。記憶装置インタフェース303は、ケーブル211を介して記憶装置210との間でデータのやり取りを行なうためのインタフェースである。表示装置304は、ユーザにメッセージを表示するためのディスプレイ等である。入力装置305は、ユーザがデータを入力するためのキーボードやマウス等である。メモリ306には、オペレーティングシステム307、アプリケーションプログラム308、及びセキュリティプログラム309等が記憶されている。

【0036】メモリ306に記憶されているオペレーティングシステム307は、ファイル管理やプロセス管理、あるいはデバイス管理といった機能を提供するために端末全体の制御を行なうプログラム群であり、ディスクバッファやキーボードバッファ等、各種ハードウェアとの間のデータのやり取りを行なうためのデータ領域を有している。アプリケーションプログラム308は、ユーザが新規ファイルの作成や既存ファイルの読み取り、書き込み等を行なう際にそれを支援・制御するプログラムである。また、セキュリティプログラム309は、ファイルの暗号化及び復号化に係る種々の処理を行なうプログラムである。

【0037】図4は、個人用記憶媒体220の内部構成図である。同図に示すように、個人用記憶媒体220には、ユーザ鍵104と呼ばれる各個人用記憶媒体に固有の秘密数値が記憶されている。

【0038】次に、図1を参照して、本実施例において、平文ファイルを暗号化する手順について簡単に説明する。

【0039】まず、アプリケーションプログラムが使用するメモリ上のデータ領域とディスクバッファとの間でデータのやり取りを行なうことができる最も小さなデータサイズに、平文ファイル100を n 分割し、 n 個の平文ブロック101、102、103を生成する。

【0040】例えば、その最小データサイズが1バイト、平文ファイルの大きさが1キロバイトである場合、その平文ファイルは1000個の平文ブロックに分割する。このデータサイズは、その端末で使用可能な全てのアプリケーションプログラムに共通であり、オペレーティングシステムの種類によって、一意に決まる大きさである。

【0041】次に、この n 個の平文ブロック101、102、103を、ユーザ鍵104でそれぞれ別々に暗号化し、 n 個の暗号文ブロック105、106、107を生成する。最後に、生成された n 個の暗号文ブロック105、106、107を連結して、暗号文ファイル108を得る。

【0042】ただし、本実施例で使用する暗号アルゴリズムは、上記データサイズの平文ブロックを同じ大きさの暗号文ブロックに変換することができる方式（例え

13

ば、平文と暗号鍵との排他的論理和を暗号文とする方式)である。

【0043】次に、図5から図7を参照して、本実施例におけるユーザの操作および端末200の処理について詳しく説明する。

【0044】図5は、端末200において、ユーザがアプリケーションプログラム308を使用して新規に作成した平文ファイルを暗号化して記憶装置210に書き込む場合の処理手順を示す流れ図である。

【0045】本処理は、ユーザが自己の個人用記憶媒体220を読み取り装置230に挿入し、アプリケーションプログラム308によって作成した平文ファイルを、記憶装置210に書き込む操作をすることによって開始される(ステップ500)。

【0046】端末200は、まず、アプリケーションプログラム308によって指定されたメモリ上のデータ領域にある平文ファイルのファイルサイズを調べ(ステップ501)、それと同じ大きさのデータ領域を新たにメモリ上に確保する(ステップ502)。そして、そのデータ領域に平文ファイルを複写する(ステップ503)。

【0047】次に、複写した平文ファイルをn個の平文ブロックに分割する(ステップ504)。平文ブロックのデータサイズは、図1で説明したように、アプリケーションプログラムが使用するメモリ上のデータ領域とディスクバッファとの間でデータのやり取りを行なうことができる最も小さなデータサイズである。このデータサイズは、オペレーティングシステムの種類によって一意に決まっている。

【0048】そして、個人用記憶媒体220よりユーザ鍵を読み取り(ステップ505)、そのユーザ鍵で、n個の平文ブロックをそれぞれ別々に暗号化する(ステップ506)。ユーザ鍵は、あらかじめ個人用記憶媒体が挿入された時点で、メモリ上の決められた領域に読み取られておいてもよい。

【0049】更に、生成されたn個の暗号文ブロックを連結し(ステップ507)、一つの暗号文ファイルとした後、本来、平文ファイルを転送するはずであったディスクバッファに、暗号文ファイルを転送して、記憶装置210に書き込む(ステップ508)。このとき、転送する暗号文ファイルのファイルサイズがディスクバッファの大きさより大きな場合には、ステップ508を繰り返し実行する。

【0050】最後に、ユーザが読み取り装置230から個人用記憶媒体220を取り出すことによって全ての処理が終了する(ステップ509)。

【0051】図6は、端末200において、ユーザがアプリケーションプログラム308を使用して既に記憶装置210に記憶されている暗号文ファイルの一部を上書きする場合の処理手順を示す流れ図である。

(8)

特開平7-140896

14

【0052】本処理は、ユーザが自己の個人用記憶媒体220を読み取り装置230に挿入し、アプリケーションプログラム308によって作成した、上書きしようとする平文データを、記憶装置210に書き込む操作をすることによって開始される(ステップ600)。

【0053】端末200は、まず、アプリケーションプログラム308によって指定されたメモリ上のデータ領域にある上書きすべき平文データのデータサイズを調べ(ステップ601)、それと同じ大きさのデータ領域を新たにメモリ上に確保する(ステップ602)。そして、そのデータ領域に平文データを複写する(ステップ603)。

【0054】次に、複写した平文データをm個の平文ブロックに分割する(ステップ604)。平文ブロックのデータサイズは、図1あるいは図5でも説明したように、アプリケーションプログラムが使用するメモリ上のデータ領域とディスクバッファとの間でデータのやり取りを行なうことができる最も小さなデータサイズである。

【0055】そして、個人用記憶媒体220よりユーザ鍵を読み取り(ステップ605)、そのユーザ鍵で、m個の平文ブロックをそれぞれ別々に暗号化する(ステップ606)。本処理でも、あらかじめ個人用記憶媒体が挿入された時点で、ユーザ鍵をメモリ上の決められた領域に読み取っておいてもよい。

【0056】更に、生成されたm個の暗号文ブロックを連結し(ステップ607)、一つの暗号文データとした後、本来、平文データを転送するはずであったディスクバッファに、暗号文データを転送して、記憶装置210に書き込む(ステップ608)。このとき、転送する暗号文データのデータサイズがディスクバッファの大きさより大きな場合には、ステップ608を繰り返し実行する。

【0057】最後に、ユーザが読み取り装置230から個人用記憶媒体220を取り出すことによって全ての処理が終了する(ステップ609)。

【0058】図7は、端末200において、ユーザがアプリケーションプログラム308を使用して既に記憶装置210に書き込まれている暗号文ファイルを読み取る場合の処理手順を示す流れ図である。

【0059】本処理は、ユーザが自己の個人用記憶媒体220を読み取り装置230に挿入し、アプリケーションプログラム308によって、記憶装置210に書き込まれている暗号文ファイルを読み取る操作をすることによって開始される(ステップ700)。

【0060】端末200は、まず、記憶装置210に記憶されている暗号文ファイルのファイルサイズを調べ(ステップ701)、それと同じ大きさのデータ領域を新たにメモリ上に確保する(ステップ702)。そして、本来、アプリケーションプログラム308によって

15

指定されたメモリ上のデータ領域に読み込まれるべき暗号文ファイルを、記憶装置210から、ディスクバッファを介して、新たに確保したデータ領域に読み取る（ステップ703）。このとき、転送する暗号文ファイルのファイルサイズがディスクバッファの大きさより大きな場合には、ステップ703の処理を繰り返して実行する。

【0061】次に、読み込まれた暗号文ファイルをn個の暗号文ブロックに分割する（ステップ704）。上述したように、本実施例で使用する暗号アルゴリズムは平文ブロックと暗号文ブロックとが同じ大きさになるような方式であるから、この暗号文ブロックのデータサイズは、図1および図5で説明したn個に分割した平文ブロックのデータサイズと同じということになる。

【0062】そして、個人用記憶媒体220よりユーザ鍵を読み取り（ステップ705）、そのユーザ鍵で暗号文ブロックをそれぞれ別々に復号する（ステップ706）。本処理でも、あらかじめ個人用記憶媒体が挿入された時点で、ユーザ鍵をメモリ上の決められた領域に読み取っておいてもよい。

【0063】更に、n個の平文ブロックを連結し（ステップ707）、一つの平文ファイルとした後、アプリケーションプログラム308によって指定されたメモリ上のデータ領域にこの平文ファイルを転送する（ステップ708）。

【0064】最後に、ユーザが読み取り装置230から個人用記憶媒体220を取り出すことによって全ての処理が終了する（ステップ709）。

【0065】上述の実施例では、平文ファイルの暗号化を行なうときに、アプリケーションプログラムの種類によって変わるような情報を使っていないので、ユーザが、その端末で利用可能な、どのようなアプリケーションプログラムを使用して平文ファイルを作成した場合においても、同じように暗号化することができる。

【0066】また、全ての平文ブロックをそれぞれ別々に暗号化しているので、各暗号文ブロックの間に相関はない。したがって、既に記憶装置に記憶されている暗号文ファイル、すなわち連結された暗号文ブロックの一部に対し、新たに作成した暗号文ブロックを上書きした場合においても、他の暗号文ブロックが破壊されることなく、元の平文ファイルに正しく復元することができる。

【0067】更に、各個人用記憶媒体毎に異なるユーザ鍵を使って暗号化を行なっているため、平文ファイルを暗号化した本人以外のユーザが、記憶装置に記憶されている暗号文ファイルを読み取って、正しい平文ファイルを手に入れることはできない。

【0068】なお、図8に示すように、個人用記憶媒体220にユーザID800（各ユーザごとに異なる個人識別子）やパスワード801をユーザ鍵104と共に記憶しておき、ユーザが個人用記憶媒体を使用する際に、

(9)

特開平7-140896

16

パスワードによる本人確認処理を行なうようにすることによって、更に安全性を高めることができる。その際、パスワードの代わりに、指紋等の各ユーザの生物学的特徴を使用して本人確認処理を行なっても同様の効果が得られる。

【0069】また、上記実施例では平文ブロックと暗号文ブロックとが同じ大きさとなるような暗号アルゴリズムを用いたが、これに限らず、平文ブロックと暗号文ブロックとが同じ大きさとならない暗号アルゴリズムを用いてもよい。この場合、平文ファイル内のデータの位置と暗号文ファイル内の位置とが、対応付けられるようになっていることが必要である。

【0070】（実施例2）次に、本発明の第2の実施例を説明する。第2の実施例は、基本的には上述の第1の実施例と同様である。そのシステム構成、及び端末の内部構成は、上述の第1の実施例の図2、3と同様である。また、個人用記憶媒体の内部構成も図4と同様である。

【0071】図9は、本実施例における平文ファイルの暗号化手順を示すブロック図である。図9において、図1と同じ処理あるいは情報には同じ番号を付して説明を省略する。図9が図1と異なる点は、ブロック900から905、及び910である。

【0072】本実施例では、各平文ブロック101、102、103を同一のユーザ鍵104で暗号化するのでなく、ユーザ鍵104と各平文ブロックに固有の値とから、平文ブロックと同じ個数のデータ鍵903、904、905を生成し、そのデータ鍵903、904、905で各平文ブロック101、102、103をそれぞれ別々に暗号化する。

【0073】平文ブロック101はデータ鍵903で暗号化し、平文ブロック102はデータ鍵904で暗号化し、…、平文ブロック103はデータ鍵905で暗号化し、というようにする。各平文ブロックに固有の値としては、例えば、同図に示すように、各平文ブロックの平文ファイルの先頭からのオフセット値900、901、902が用いられる。

【0074】図10は、端末200において、ユーザがアプリケーションプログラム308を使用して新規に作成した平文ファイルを、暗号化して記憶装置210に書き込む場合の処理手順を示す流れ図である。これは基本的には図5と同様の手順である。

【0075】ただし、個人用記憶媒体220、あるいはメモリ上の決められたデータ領域からユーザ鍵を読み取った（ステップ505）後、そのユーザ鍵と各平文ブロックの平文ファイルの先頭からのオフセット値より、n個のデータ鍵を生成し（ステップ1000）、そのn個のデータ鍵でn個の平文ブロックをそれぞれ別々に暗号化する（ステップ1001）、という点が異なる。

【0076】図11は、端末200において、ユーザが

17

アプリケーションプログラム308を使用して、既に記憶装置210に記憶されている暗号文ファイルの一部を上書きする場合の処理手順を示す流れ図である。これは基本的には図6と同様の手順である。

【0077】ただし、個人用記憶媒体220、あるいはメモリ上の決められたデータ領域からユーザ鍵を読み取った(ステップ605)後、そのユーザ鍵と各平文ブロックの平文ファイルの先頭からのオフセット値より、m個のデータ鍵を生成し(ステップ1100)、そのm個のデータ鍵でm個の平文ブロックをそれぞれ別々に暗号化する(ステップ1101)、という点と異なる。

【0078】本実施例では、データ鍵を生成するために上書きすべきデータの先頭からのオフセット値ではなく、元の平文ファイルの先頭からのオフセット値を使用している。したがって、ここで使用するm個のデータ鍵の値は、上書きする位置に記憶されている元の暗号文ブロックを生成するときに使用したデータ鍵の値と同じであることは明らかである。

【0079】図12は、端末200において、ユーザがアプリケーションプログラム308を使用して、既に記憶装置210に記憶されている暗号文ファイルを読み取る場合の処理手順を示す流れ図である。これは基本的には図7と同様の手順である。

【0080】ただし、個人用記憶媒体220、あるいはメモリ上の決められたデータ領域からユーザ鍵を読み取った(ステップ705)後、そのユーザ鍵と各暗号文ブロックの暗号文ファイルの先頭からのオフセット値(平文ファイルの先頭からのオフセット値と同じ値)より、n個のデータ鍵を生成し(ステップ1200)、そのn個のデータ鍵でn個の暗号文ブロックをそれぞれ別々に復号する(ステップ1201)、という点と異なる。

【0081】第1の実施例では、各平文ブロックを同一のユーザ鍵で暗号化していた。これに対し、本実施例では、一つのユーザ鍵から平文ブロックと同数のデータ鍵を生成し、そのデータ鍵で各平文ブロックをそれぞれ別々に暗号化している。したがって、第1の実施例と同様の効果が得られるほかに、個人用記憶媒体に記憶する情報を変更しなくても、同一の平文ブロックが必ず同一の暗号文ブロックに変換されるということがなくなるので、平文ファイルを転送されにくくすることができる。

【0082】(実施例3)次に、本発明の第3の実施例を説明する。第3の実施例は、基本的には上述の第2の実施例と同様である。ただし、各端末が通信網を介して相互に接続されており、アプリケーションプログラムを使って作成したファイルを、別の端末の記憶装置に書き込むことが可能である点と異なる。

【0083】図13は、本実施例のシステム構成を示すブロック図である。

【0084】図13において、一つ一つの端末と、それと共に使用される記憶装置、読み取り装置、及び個人用

(10)

特開平7-140896

18

記憶媒体は、基本的に図2のそれと同じである。ただし、複数の端末200が通信網1300によって相互に接続されている点と異なる。

【0085】図14は、本実施例の端末の内部構成を示すブロック図である。これは基本的に図3と同じである。ただし、端末200が、通信網1300を介して別の端末との間でデータのやり取りを行なうための通信網インタフェース1400を有している点と、メモリ306にそれを制御するための通信制御プログラム1401が記憶されている点とが異なる。

【0086】図15は、端末200において、ユーザがアプリケーションプログラム308を使用して新規に作成した平文ファイルを、暗号化して、別の端末の記憶装置210に書き込む場合の処理手順を示す流れ図である。これは基本的には図10と同様の手順である。ただし、ディスクバッファではなく、通信バッファを介して、別の端末の記憶装置210に暗号文ファイルを書き込む点と異なっている(ステップ1500)。

【0087】図16は、端末200において、ユーザがアプリケーションプログラム308を使用して、既に別の端末の記憶装置210に記憶されている暗号文ファイルの一部を上書きする場合の処理手順を示す流れ図である。これは基本的には図11と同様の手順である。ただし、ディスクバッファではなく、通信バッファを介して、別の端末の記憶装置210に暗号文データを上書きする点と異なっている(ステップ1600)。

【0088】図17は、端末200において、ユーザがアプリケーションプログラム308を使用して、既に別の端末の記憶装置210に記憶されている暗号文ファイルを読み取る場合の処理手順を示す流れ図である。これは基本的には図12と同様の手順である。ただし、ディスクバッファではなく、通信バッファを介して、別の端末の記憶装置210から暗号文ファイルを読み取る点と異なっている(ステップ1700)。

【0089】本実施例では、通信バッファに転送される以前にデータが暗号化されているので、通信網には暗号化されたデータだけが流れることになる。したがって、第2の実施例と同様の効果が得られるほかに、通信網を介して別の端末の記憶装置にファイルを書き込むような場合にも、自端末の場合と同様の安全性を確保することができる。

【0090】

【発明の効果】以上説明したように、本発明によれば、アプリケーションプログラムによって指定されたメモリ上のデータ領域からディスクバッファにデータを転送することができる最も小さなデータサイズと同じ大きさ(オペレーティングシステムの種別によって一意に決まる大きさ)でファイルを暗号化しているため、使用するアプリケーションの種類に依らず、例えば、そのアプリケーションプログラムが、既に記憶装置に記憶されてい

19

る暗号文ファイルの一部を上書きした場合でも、元の平文ファイルに正しく復元することができる。

【0091】また、各平文ブロックを、それらの平文ブロックと同じ個数のデータ鍵で暗号化した場合には、同一の平文ブロックが、必ずしも同一の暗号文ブロックには変換されないで、平文ファイルを乱雑されにくくなり、安全性を高めることができる。

【0092】更に、アプリケーションプログラムによって指定されたメモリ上のデータ領域にある平文ファイルが、通常バッファに転送されたときには既に暗号化されているので、通信網には暗号文ファイルが流れることになり、通信網を介して別の端末の記憶装置に暗号文ファイルを書き込む場合にも、自端末の記憶装置に書き込む場合と同様の安全性を確保することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施例を示すブロック図である。

【図2】第1の実施例のシステム構成図である。

【図3】第1の実施例における端末の内部構成図である。

【図4】第1の実施例における個人用記憶媒体の内部構成図である。

【図5】第1の実施例において、新規に作成した平文ファイルを暗号化する場合の処理手順を示す流れ図である。

【図6】第1の実施例において、記憶装置に記憶された暗号文ファイルに上書きする場合の処理手順を示す流れ図である。

【図7】第1の実施例において、暗号文ファイルを復号する場合の処理手順を示す流れ図である。

(11)

特開平7-140896

20

【図8】第1の実施例の変形例における個人用記憶媒体の内部構成図である。

【図9】本発明の第2の実施例を示すブロック図である。

【図10】第2の実施例において、新規に作成した平文ファイルを暗号化する場合の処理手順を示す流れ図である。

【図11】第2の実施例において、記憶装置に記憶された暗号文ファイルに上書きする場合の処理手順を示す流れ図である。

【図12】第2の実施例において、暗号文ファイルを復号する場合の処理手順を示す流れ図である。

【図13】本発明の第3の実施例のシステム構成図である。

【図14】第3の実施例における端末の内部構成図である。

【図15】第3の実施例において、新規に作成した平文ファイルを暗号化する場合の処理手順を示す流れ図である。

【図16】第3の実施例において、記憶装置に記憶された暗号文ファイルに上書きする場合の処理手順を示す流れ図である。

【図17】第3の実施例において、暗号文ファイルを復号する場合の処理手順を示す流れ図である。

【符号の説明】

200…端末、

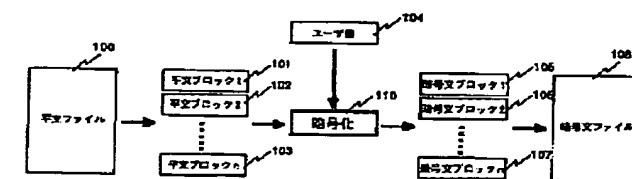
210…記憶装置、

220…個人用記憶媒体、

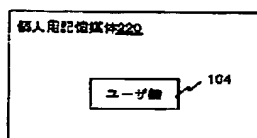
230…読み取り装置、

1300…通信網。

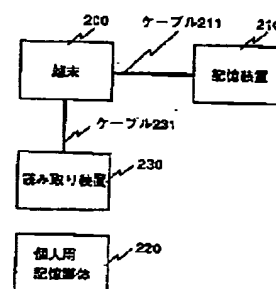
【図1】



【図4】



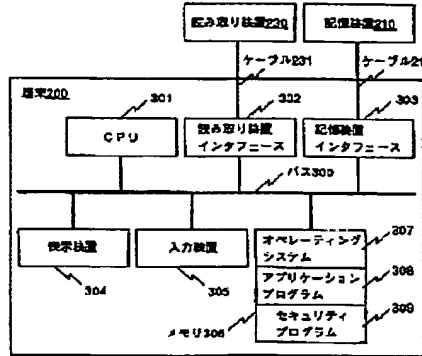
【図2】



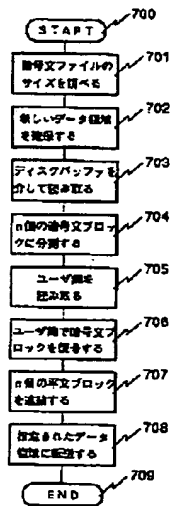
(12)

特開平7-140896

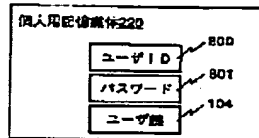
【図3】



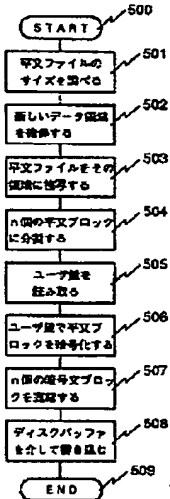
【図7】



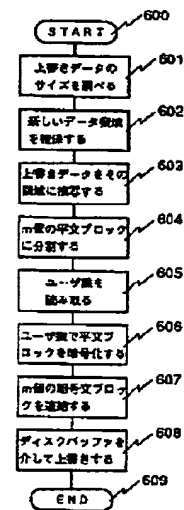
【図8】



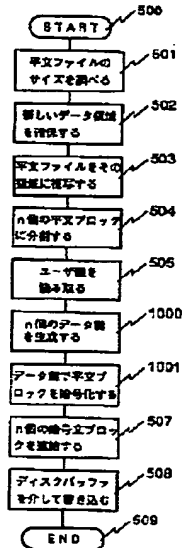
【図5】



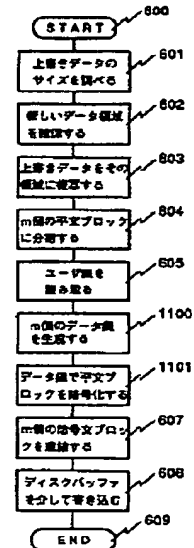
【図6】



【図10】



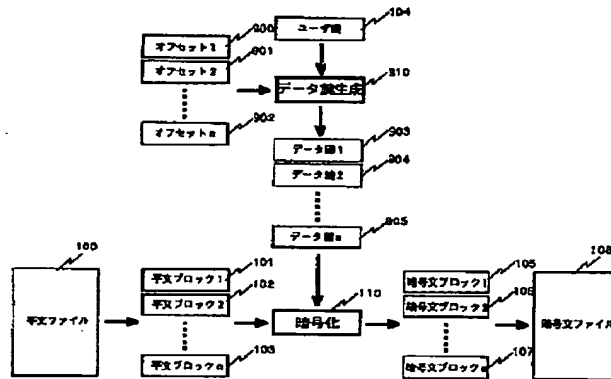
【図11】



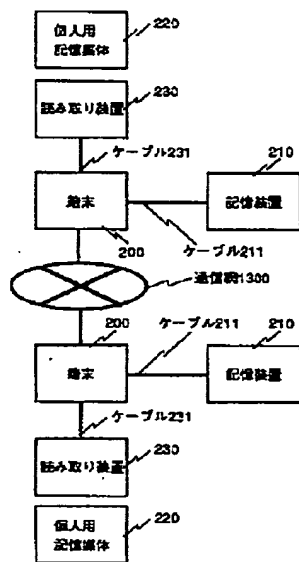
(13)

特開平7-140896

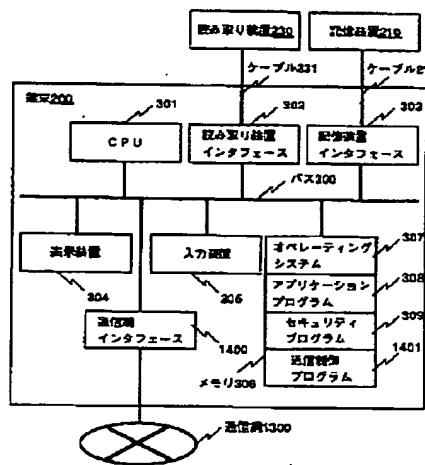
【図9】



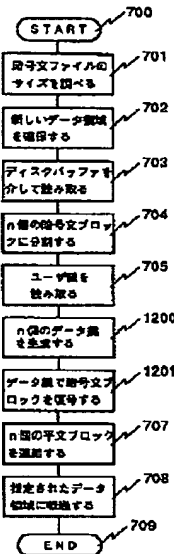
【図13】



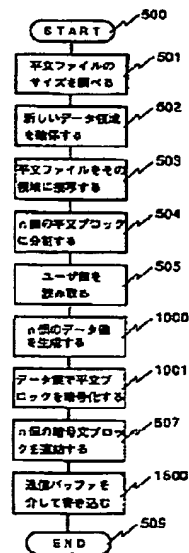
【図14】



【図12】



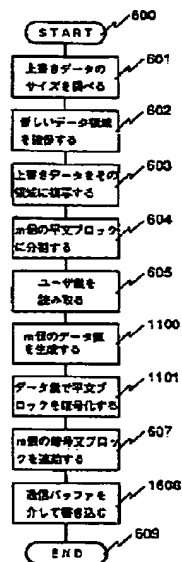
【図15】



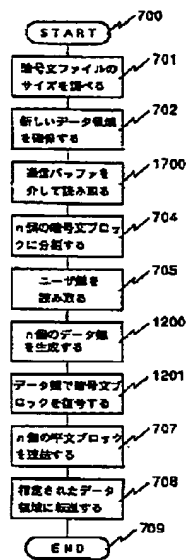
(14)

特開平7-140896

【図16】



【図17】



フロントページの続き

(72) 発明者 宝木 和夫
神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内

(72) 発明者 中村 輝雄
神奈川県横浜市中央区尾上町6丁目81番地
日立ソフトウェアエンジニアリング株式会
社内

(72) 発明者 納富 雅人
神奈川県横浜市中央区尾上町6丁目81番地
日立ソフトウェアエンジニアリング株式会
社内